CLAIMS

1. A content reproduction system comprising:

a content distribution apparatus operable to distribute an encrypted content, which is generated by encrypting a content using a content key uniquely assigned to the content, and an encrypted content key which is generated by encrypting the content key using a master key that is commonly assigned to a plurality of contents including the content;

a content-use recording medium in which master information, which is generated from a source material that includes at least the master key, is recorded; and

a reproduction apparatus operable to acquire the encrypted content and the encrypted content key from the content distribution apparatus, generate a master key from the master information recorded in the content-use recording medium, generate a content key by decrypting the encrypted content key using the generated master key, generate a content by decrypting the encrypted content using the generated content key, and reproduce the generated content.

2. The content reproduction system of Claim 1, wherein

the master information is an encrypted master key that is generated by encrypting the master key using a device key uniquely assigned to the reproduction apparatus, and

the reproduction apparatus generates a master key by

decrypting the encrypted master key using a device key uniquely assigned to the reproduction apparatus.

3. A reproduction apparatus that acquires encrypted contents from a content distribution apparatus and reproduces contents that are generated by decrypting the acquired encrypted contents, comprising:

a content information acquiring unit operable to acquire an encrypted content, which is generated by encrypting a content using a content key uniquely assigned to the content, and an encrypted content key which is generated by encrypting the content key using a master key that is commonly assigned to a plurality of contents including the content, from the content distribution apparatus;

a content key generating unit operable to generate a master key from master information recorded in a content-use recording medium, the master information being generated from a source material that includes at least the master key commonly assigned to the plurality of contents, and generate a content key by decrypting the encrypted content key using the generated master key;

a content generating unit operable to generate a content by decrypting the encrypted content using the generated content key; and

a reproducing unit operable to reproduce the generated content.

4. The reproduction apparatus of Claim 3, wherein

the master information recorded in the content-use recording medium is an encrypted master key that is generated by encrypting the master key using a device key uniquely assigned to the reproduction apparatus, and

the content key generating unit generates a master key by decrypting the encrypted master key using a device key uniquely assigned to the reproduction apparatus.

5. The reproduction apparatus of Claim 4, wherein

the content-use recording medium further stores therein another encrypted master key that is generated by encrypting another master key using the device key uniquely assigned to the reproduction apparatus, and

the content key generating unit further generates the other master key by decrypting the other encrypted master key using the device key, and generates a content key by decrypting the encrypted content key using the generated other master key.

6. The reproduction apparatus of Claim 3, wherein

the master information is an encrypted master key set that is generated by encrypting, using the device key uniquely assigned to the reproduction apparatus, a master key set composed of the master key and another master key, and

the content key generating unit generates the master key and the other master key by decrypting the encrypted master key set using the device key, and generates a content key by decrypting

the encrypted content key using the generated master key.

7. The reproduction apparatus of Claim 3, wherein

the content-use recording medium further stores therein use period information in association with the master information, the use period information indicating a use period of the content,

the content information acquiring unit includes:

an acquisition information receiving sub-unit operable to receive acquisition information that indicates either rental, which means that the content is acquired for rent, or purchase which means that the content is acquired for purchase; and

an acquisition information storage sub-unit operable to store therein the received acquisition information in association with the encrypted content and the encrypted content key,

the content key generating unit includes:

an acquisition information judging sub-unit operable to judge whether the received acquisition information indicates rental or purchase; and

a reproduction control sub-unit operable to permit a reproduction of the content if the acquisition information judging sub-unit judges that the acquisition information indicates purchase, and permit a reproduction of the content if the acquisition information judging sub-unit judges that the acquisition information indicates rental, and if a requested use period for the content is within the use period indicated by the use period information.

8. The reproduction apparatus of Claim 7, wherein

the reproduction control sub-unit includes:

a reproduction instruction receiving lower-unit operable to receives a reproduction instruction for the content; and

a period judging lower-unit operable to, if the acquisition information judging sub-unit judges that the acquisition information indicates rental, calculate a period between acquisition of the encrypted content and the encrypted content key and reception of the reproduction instruction, and judge whether the calculated period is within the use period indicated by the use period information.

9. The reproduction apparatus of Claim 7, wherein

the content-use recording medium further stores therein usable content information that indicates a condition for using the content, and

the content information acquiring unit judges whether the condition for using the content is satisfied, acquires the encrypted content and the encrypted content key from the content distribution apparatus if having judged that the condition for using the content is satisfied, and does not acquire the encrypted content and the encrypted content key from the content distribution apparatus if having judged that the condition is not satisfied.

10. The reproduction apparatus of Claim 9, wherein

the content distribution apparatus distributes the encrypted content and the encrypted content key to the reproduction

apparatus regardless of whether the content distribution apparatus receives a content distribution request from the reproduction apparatus or not, and

the content information acquiring unit receives the encrypted content and the encrypted content key from the content distribution apparatus, and judges whether the received encrypted content and encrypted content key satisfy the condition indicated by the usable content information, holds the received encrypted content and encrypted content key if having judged that the received encrypted content and encrypted content key satisfy the condition, and discards the received encrypted content and encrypted content key if having judged that the received encrypted content and encrypted content key do not satisfy the condition.

11. A content-use recording medium which stores therein:

use period information which indicates a use period of a content; and

master information which is generated from a source material that includes at least a master key that is commonly assigned to a plurality of contents including the content, the master key being used for encrypting a content key, the master information being associated with the use period information in the content-use recording medium.

12. The content-use recording medium of Claim 11 further storing therein usable content information that indicates a condition for using the content, the usable content information being associated

with the master information in the content-use recording medium.

13. The content-use recording medium of Claim 11, wherein the master information is an encrypted master key that is generated by encrypting the master key using a device key uniquely assigned to a reproduction apparatus for reproducing the content.

14. The content-use recording medium of Claim 13 further storing therein another encrypted master key that is generated by encrypting another master key using the device key uniquely assigned to the reproduction apparatus, the other encrypted master key being associated with another piece of use period information.

15. The content-use recording medium of Claim 11, wherein

the master information is an encrypted master key set that is generated by encrypting, using the device key uniquely assigned to the reproduction apparatus, a master key set composed of the master key and another master key.

16. A content distribution apparatus connected to a reproduction apparatus via a network, comprising:

a content information storage unit storing therein an encrypted content, which is generated by encrypting a content using a content key uniquely assigned to the content, and an encrypted content key which is generated by encrypting the content key using a master key that is commonly assigned to a plurality of contents including the content; and

a distributing unit operable to distribute the encrypted content and the encrypted content key stored in the content information storage unit to the reproduction apparatus via the network.

17. The content distribution apparatus of Claim 16 further comprising:

a master key storage unit storing therein a plurality of master keys;

a state changing unit operable to, if any of the plurality of master keys is not permitted to be used, set the not-permitted master key to an unusable state; and

a content key encrypting unit operable to generate one or more encrypted content keys respectively using one or more master keys that are permitted to be used, among the plurality of master keys.

18. A data writing apparatus for writing data into a content-use recording medium, comprising:

a master key generating unit operable to generate a master key that is commonly assigned to a plurality of contents, the master key being used for encrypting a content key;

a master information generating unit operable to generate master information that indicates the master key; and

a writing unit operable to write the generated master information into the content-use recording medium.

19. A content reproduction method for use in a reproduction apparatus that acquires encrypted contents from a content distribution apparatus and reproduces contents that are generated by decrypting the acquired encrypted contents, the content reproduction method comprising the steps of:

acquiring an encrypted content, which is generated by encrypting a content using a content key uniquely assigned to the content, and an encrypted content key which is generated by encrypting the content key using a master key that is commonly assigned to a plurality of contents including the content, from the content distribution apparatus;

generating a master key from master information recorded in a content-use recording medium, the master information being generated from a source material that includes at least the master key commonly assigned to the plurality of contents, and generating a content key by decrypting the encrypted content key using the generated master key;

generating a content by decrypting the encrypted content using the generated content key; and

reproducing the generated content.

20. A content reproduction program for use in a reproduction apparatus that acquires encrypted contents from a content distribution apparatus and reproduces contents that are generated by decrypting the acquired encrypted contents, the content reproduction program comprising the steps of:

acquiring an encrypted content, which is generated by

encrypting a content using a content key uniquely assigned to the content, and an encrypted content key which is generated by encrypting the content key using a master key that is commonly assigned to a plurality of contents including the content, from the content distribution apparatus;

generating a master key from master information recorded in a content-use recording medium, the master information being generated from a source material that includes at least the master key commonly assigned to the plurality of contents, and generating a content key by decrypting the encrypted content key using the generated master key;

generating a content by decrypting the encrypted content using the generated content key; and

reproducing the generated content.

21A computer-readable recording medium recording therein a content reproduction program for use in a reproduction apparatus that acquires encrypted contents from a content distribution apparatus and reproduces contents that are generated by decrypting the acquired encrypted contents, the content reproduction program comprising the steps of:

acquiring an encrypted content, which is generated by encrypting a content using a content key uniquely assigned to the content, and an encrypted content key which is generated by encrypting the content key using a master key that is commonly assigned to a plurality of contents including the content, from the content distribution apparatus;

generating a master key from master information recorded in a content-use recording medium, the master information being generated from a source material that includes at least the master key commonly assigned to the plurality of contents, and generating a content key by decrypting the encrypted content key using the generated master key;

generating a content by decrypting the encrypted content using the generated content key; and

reproducing the generated content.